Enclosure 7

Somerset
NHS Foundation Trust

Report Details	
Subject	Information Governance Annual Report
Quarter	Annual Report 2020/21
Author/Lead	Louise Coppin
Date of Meeting	20 October 2021
Audit and Measurement	Data Security and Protection Toolkit
External Assurance	Data Security and Protection Toolkit Information Commissioner's Office
Issues/Risks	

Introduction

The DSPT is an online self-assessment tool that allows organisation to measure their performance against the National Data Guardians 10 Data Security Standards (including cyber security).

All organisations that have access to NHS patient data and systems must use this toolkit to provide assurance that they are practicing good data security and that personal information is handled correctly.

The information governance team integrated during 2019/20 in preparation for the merger of Taunton and Somerset NHS Foundation and Somerset Partnership NHS Foundation Trusts and was therefore in a good position for the merger in April 2020. This included the appointment of a single Data Protection Officer as well as a single Caldicott Guardian and SIRO, working across the legacy trusts in advance of the merger. Preparatory work included review of all working practices, preparation of new policies and other documentation and updating intranet and internet sites, reviews of how we log and respond to Freedom of Information requests, subject access requests, data subjects rights, how we deal with incidents and how we manage data protection impact assessments, all of which are required by data protection and FOI laws.

Data Security and Protection Toolkit

An internal Audit of our Data Security and Protection Toolkit submission was undertaken by BDO in December 2020 achieving a 'substantial level of assurance'

The final assessment of the Data Security and Protection toolkit was submitted in June 2021 with a level of Standards Exceeded (Appendix 1), the highest level of attainment.

Incidents

	Q1	Q2	Q3	Q4	Total
Total Number of Data Security Incidents Reported *all incidents are not necessarily data protection breaches	**75**	**81**	**231**	**192**	**579***
Incidents reported to the ICO	**0**	**1**	**1**	**1**	**3**
Data sent by email to incorrect recipient	11	17	26	14	
Data posted to incorrect recipient	6	12	6	16	
Data faxed/printed to incorrect recipient	1		1		
Data sent by unencrypted email	2				
Failure to redact data	2	1		1	
Verbal disclosure	5	1	7	4	
Failure to use bcc when sending email		1		1	
Loss or theft of paperwork	4	6	20	4	
Use of unmanaged personal mobile/email to process Trust data	1	1	2	2	
Insecure storage of paperwork	8	2	7	18	
Insecure disposal of paperwork	2		2		
Other security failing	5	7	35	14	
Records accessed inappropriately	3	5	3	2	
Area Left Insecure	8	16	43	35	
IT system failure		2		2	
Wrong patient identification	17	10	53	16	
Inaccurate/incomplete record keeping			26	63	

All incidents are reviewed by the IG team and consideration given as to whether the data subject should be informed of the incident and whether we need to report to the ICO.

We contact the reporter for each of these incidents to identify what went wrong, do we need to review any processes to prevent this happening again, and are staff fully trained.

The following incidents were reported to the ICO:

Staff member discovered that her son's toy had a recording device inserted inside it (toy was a present from her ex-husband). Staff member has been working from home since March, and may have discussed clients on the telephone, and conference calls, which may have been recorded on the device resulting in client confidentiality	Closed. ICO response: breach notification obligation does not apply to the incident you have described	Confirmed that device was a GPS tracking device and not a recording device as originally thought.
AAA Screening team sent an email to the Practice Manager at Burnham and Berrow Medical Centre which contained details of 14 patients. The Practice Manager inadvertently forwarded the email (which contained details of 14 patients) to one of their patients. (Patient already has a grievance with the medical centre and had no link with the AAA screening team).	Closed. No further action from ICO	
A patient's discharge summary was accidently mixed up in another patient's paperwork. This bundle of paperwork was then given to a patient and once they arrived home they realised that it contained the document which relates to another individual. The incorrect recipient of this document contacted the patient it related to via Facebook to inform them of what had happened	Closed. No further action from ICO	

Subject Access Requests

	Q1	Q2	Q3	Q4	Total
Number Received	473	556	606	620	2255
Responded within timescales	95.18%	95.5%	88.3%	39.0%	80.22%
Reviews	0	0	0	0	0
Reports to the ICO	0	1	0	0	0

There was a significant decline in the compliance rate for responding to SARs during Q4 due to:

- Increase in requests Q3 and Q4.
- 3 new staff requiring training during Q4
- Delay in obtaining log ins for new staff to IT systems
- Sickness and high annual leave during Q4
- More data systems to check (ie legacy systems from the two Trusts has had an impact on the time it takes to deal with each request)

The Data Access and Disclosure Office also took on the role of providing Mental Health records for Tribunals which had a significant impact to the workload. (This work had previously seen solicitors come to view the records on site, which they were unable to do during COVID restrictions).

Data Subjects Rights

Under Data Protection Law, data subjects have the right to make requests for rectification, erasure and restriction to their records. These rights are not absolute each needs to be investigated on its own merits.

	Total	**Result**
Rectification	8	5 upheld 3 not upheld
Erasure	0	N/A
Restriction	0	N/A

Data Security and Protection Training

	SFT Acute	**SFT MH/Com**	**SFT**
April	87%	90%	
May	89%	93%	
June	*Not available*	*Not available*	*Not available*
July			85.4%
August			85.2%
September			89.4%
October			89.5%
November			90.5%
December			90.1%
January			90.4%
February			90.7%
March			90.9%

These figures have increased significantly since July 2018 when TST only achieved 46% compliance.

The above figures relate to the online Data Security training course, however, there are other sources of training including:

- Regular updates within staff bulletins
- Paper version for cleaning staff and estates workers
- Ad hoc training sessions within departments and teams

The Data Security and Protection Toolkit has a requirement to have 95% compliance – which we did reach for the June 2021 submission.

FOI Requests

	Q1	Q2	Q3	Q4	Total
Number received	99	131	162	148	504
Responded to within timescales	85.32%	75.63%	87.7%	89.74%	
Reports to ICO	0	0	0	0	

National Data Opt Out Compliance

The national data opt-out was introduced on 25 May 2018, enabling patients to opt out from the use of their data for research or planning purposes, in line with the recommendations of the National Data Guardian in her Review of Data Security, Consent and Opt-Outs.

Patients can view or change their national data opt-out choice at any time by using the online service at www.nhs.uk/your-nhs-data-matters or by clicking on "Your Health" in the NHS App, and selecting "Choose if data from your health records is shared for research and planning". Compliance with the National Data Opt out was originally due by 31 March 2020, however due to the Covid-19 outbreak, NHS digital extended the compliance date to 30 September 2020. This has been moved again a number of times and the current compliance date is expected to be 30 March 2022.

We have identified a number of flows of information which are for research and planning purposes, where Section 251 of the Health and Social Care Act 2012 (ie approval provided by the Confidentiality Advisory Board) as these are the only flows of information that the NDOO affects.

Our information services team have confirmed that technology is in place to accommodate this via the MESH system which will transfer a list of NHS numbers to NHS digital to enable them to strip out those patients who have opted out of secondary use of their information.

Data Protection Impact Assessments (DPIAs)

DPIAs are legally required under the Data Protection Act 2018 when we have a high risk processing of large amounts of data. We received 73 DPIAs during this period. Some of these relate to new systems being implemented, sharing data with a different organisation, or working in a different way.

Sensyne

Work is ongoing with developing an information sharing agreement with Sensyne enable the ethical application of clinical artificial intelligence research on anonymised patient data to improve patient care and accelerate research into new medicines.

Where patients have signed up to the national data opt out, we will be removing their data prior to anonymisation and their data will not be included in the dataset provided to Sensyne.

What's happening in 2021/22

Work has started to bring the information governance/data protection and medical records teams together for the impending merger with Yeovil District Hospital. This will include review of all documentation (policies, procedures, guidance) to bring in line with legal requirements and best practice.

Somerset NHS Foundation Trust
Data Security and Protection Toolkit

For the Period of April 2020 to June 2021
Final Submission June 2021

The DSPT is an online self-assessment tool that allows organisation to measure their performance against the National Data Guardians 10 Data Security Standards.

All organisations that have access to NHS patient data and systems must use this toolkit to provide assurance that they are practicing good data security and that personal information is handled correctly.

Data Security Standard 1: All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is only shared for lawful and appropriate purposes

Data Security Standard 2: All staff understand their responsibilities under the National Data Guardian's Data Security Standards, including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches.

Data Security Standard 3: All staff complete appropriate annual data security training and pass a mandatory test, provided through the revised Information Governance Toolkit. Leadership Obligation 2: Process: ensure the organisation proactively prevents data security breaches and responds appropriately to incidents or near misses.

Data Security Standard 4: Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All access to personal confidential data on IT systems can be attributed to individuals.

Data Security Standard 5: Processes are reviewed at least annually to identify and improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise data security.

Data Security Standard 6: Cyber-attacks against services are identified and resisted and CareCERT security advice is responded to. Action is taken immediately following a data breach or a near miss, with a report made to senior management within 12 hours of detection.

Data Security Standard 7: A continuity plan is in place to respond to threats to data security, including significant data breaches or near misses, and it is tested once a year as a minimum, with a report to senior management. Leadership Obligation 3: Technology: ensure technology is secure and up-to-date.

Data Security Standard 8: No unsupported operating systems, software or internet browsers are used within the IT estate.

Data Security Standard 9: A strategy is in place for protecting IT systems from cyber threats which is based on a proven cyber security framework such as Cyber Essentials. This is reviewed at least annually.

Enclosure 7

Data Security Standard 10: IT suppliers are held accountable via contracts for protecting the personal confidential data they process and meeting the National Data Guardian's Data Security Standards.

Updated Toolkit

The revised assertions we made available in November 2020, significantly delayed due to Covid-19.

Changes have been made to the new toolkit in order to:

- Respond to lessons learned and direct feedback from users following the second year of the DSPT.
- Make "Cyber Essentials" requirements mandatory for relevant organisations in 2020-21.
- Rationalise the evidence items which are now considered "business as usual" or where there is overlap between evidence items.

Audit

Our toolkit was audited by BDO in March 2021 using the new criteria provided by NHSX for auditing the DSPT including a set list of assertions.

The Audit found that the evidence provided for 31 of the 40 mandatory sub-assertions was found to be satisfactory and in line with the requirements of the independent assessment framework.

There was insufficient evidence to completely support, at the time of the audit, 9 of the 40 mandatory sub-assertions included in the sample. A compliance score of 78% was provided.

Detailed findings and recommendations (page 4) and the management response (page 8) can be found within the attached report.

SFT Data Security
and Protection Tool

Required Submissions

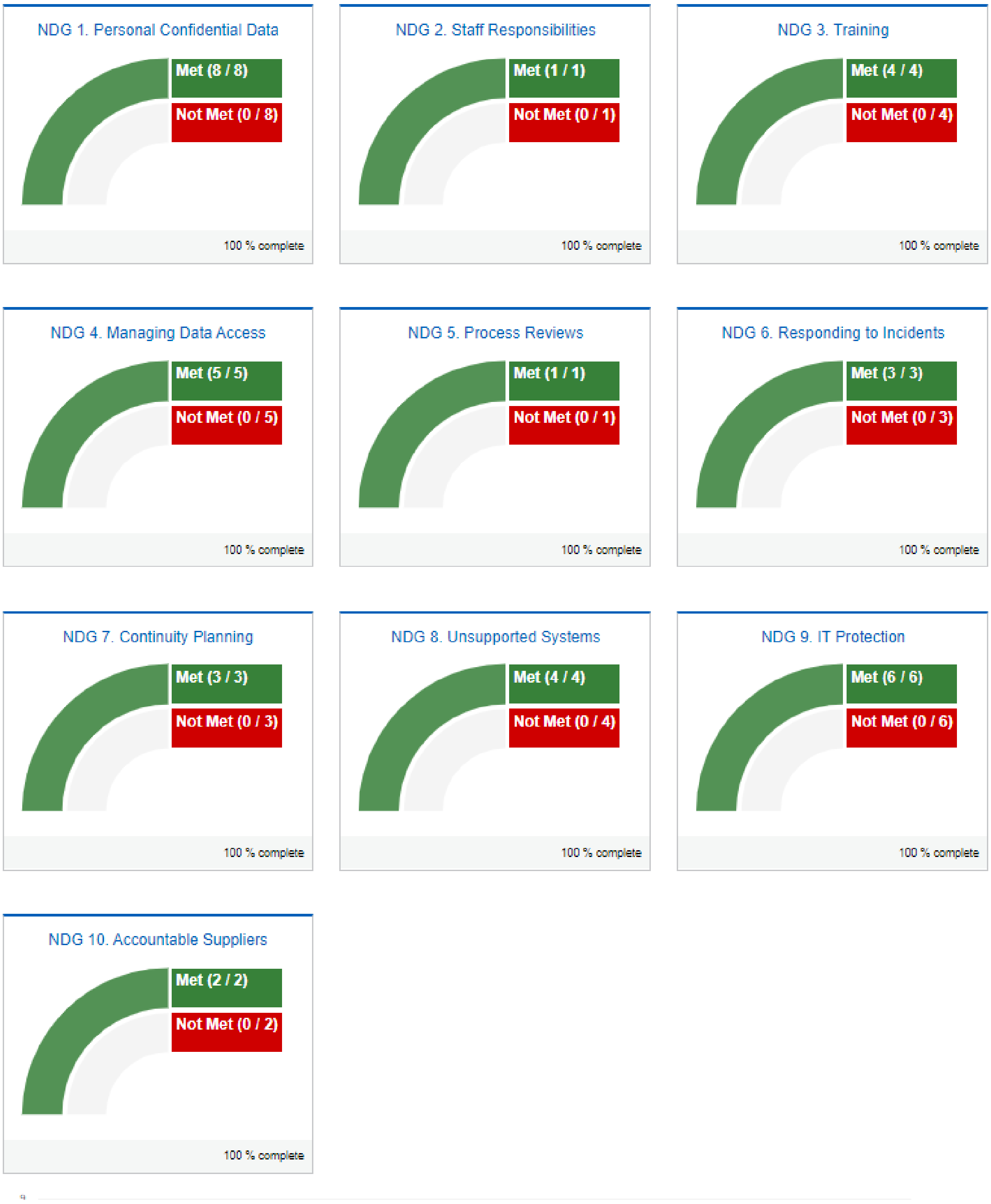
- The baseline was submitted in February 2021
- The final submission will be due in June 2021

Assessment Progress

Our current assessment shows:

- 110 of 110 mandatory evidence items provided
- 42 of 42 assertions confirmed.
- Current status is 'Standards Exceeded'

Our toolkit is therefore in a fit state for submission.



NDG 1. Personal Confidential Data
Met (8 / 8)
Not Met (0 / 8)
100 % complete

NDG 2. Staff Responsibilities
Met (1 / 1)
Not Met (0 / 1)
100 % complete

NDG 3. Training
Met (4 / 4)
Not Met (0 / 4)
100 % complete

NDG 4. Managing Data Access
Met (5 / 5)
Not Met (0 / 5)
100 % complete

NDG 5. Process Reviews
Met (1 / 1)
Not Met (0 / 1)
100 % complete

NDG 6. Responding to Incidents
Met (3 / 3)
Not Met (0 / 3)
100 % complete

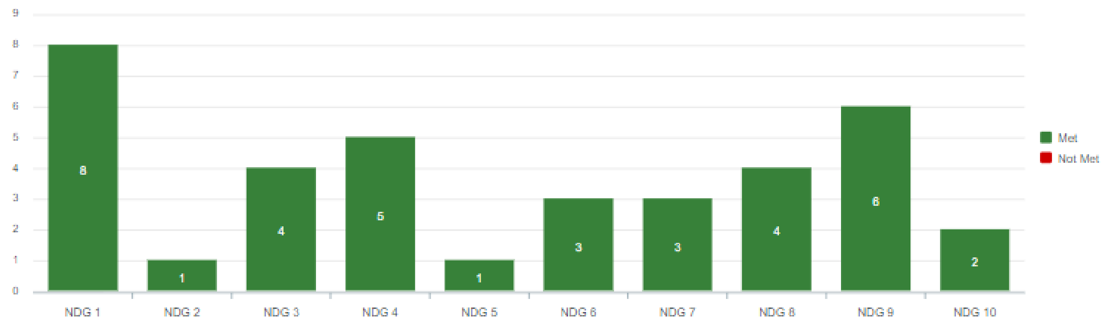
NDG 7. Continuity Planning
Met (3 / 3)
Not Met (0 / 3)
100 % complete

NDG 8. Unsupported Systems
Met (4 / 4)
Not Met (0 / 4)
100 % complete

NDG 9. IT Protection
Met (6 / 6)
Not Met (0 / 6)
100 % complete

NDG 10. Accountable Suppliers
Met (2 / 2)
Not Met (0 / 2)
100 % complete

Enclosure 7



NDG 1 - Personal Confidential Data
NDG 3 - Training
NDG 5 - Process Reviews
NDG 7 - Continuity Planning
NDG 9 - IT Protection

NDG 2 - Staff Responsibilities
NDG 4 - Managing Data Access
NDG 6 - Responding to Incidents
NDG 8 - Unsupported Systems
NDG 10 - Accountable Suppliers

Final Report

Somerset NHS FT
RH5 DSPT as at 18 Ju

Approval for Submission

Signed:
Date: 18 June 2021

Louise Coppin
Head of Information Governance & Data Protection Officer

Signed:
Date: 18 June 2021

David Shannon
Director of Stategic Development & SIRO